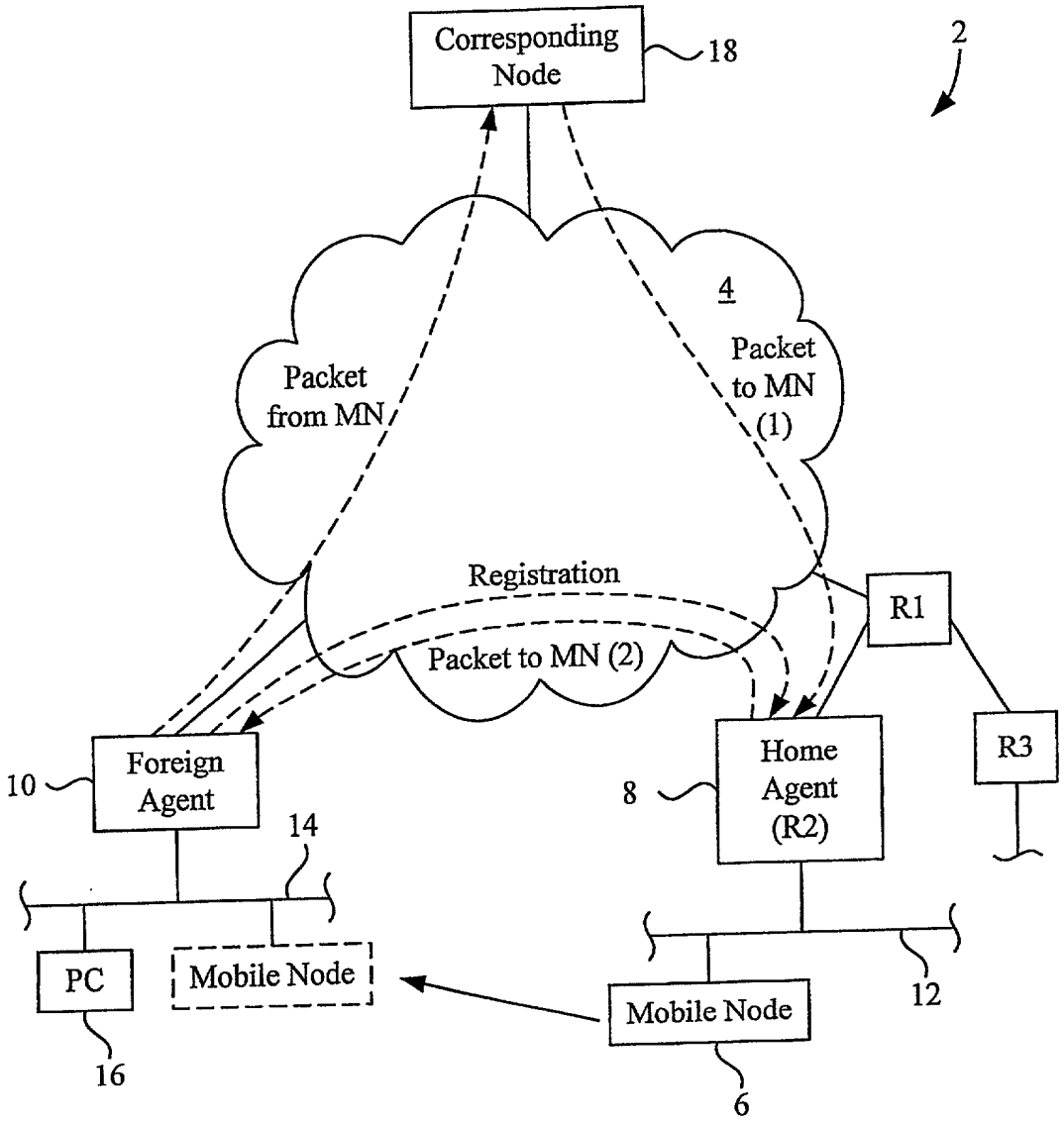

Corresponding Node
18
2
4
Packet from MN
Packet to MN (1)
Registration
Packet to MN (2)
R1
R3
Home Agent (R2)
8
Foreign Agent
10
14
PC
Mobile Node
16
Mobile Node
6
12

FIGURE 1A

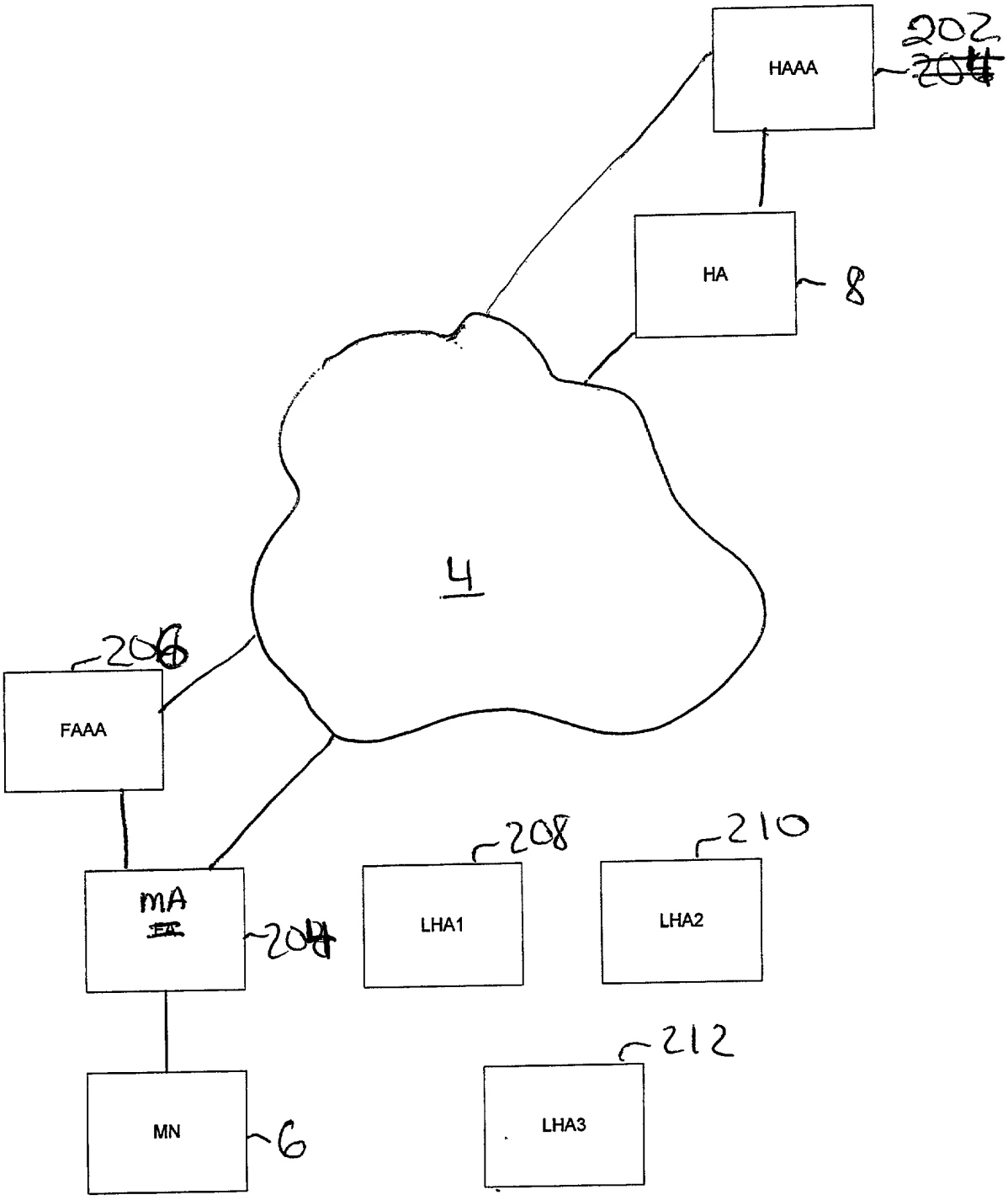
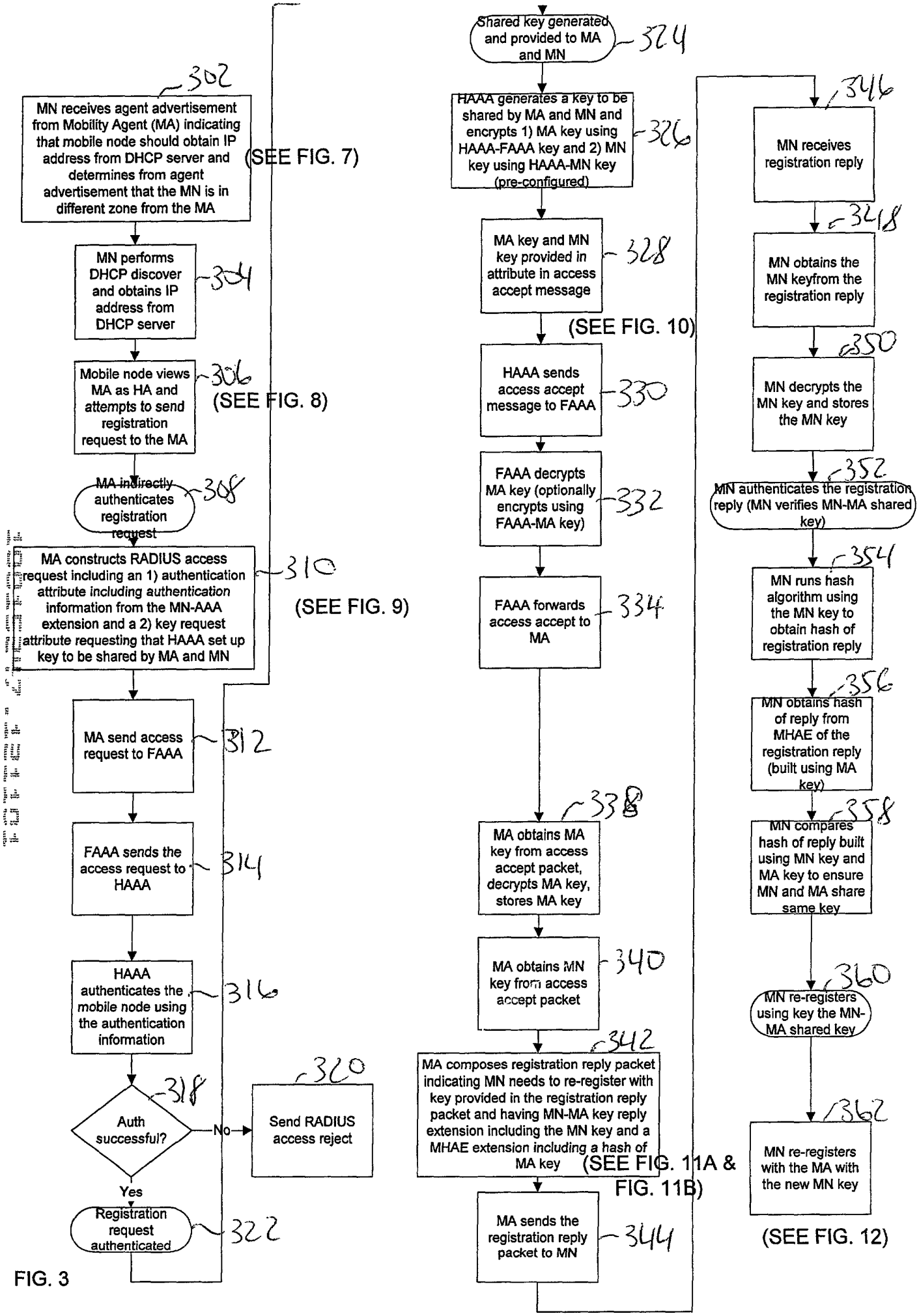


FIG. 2


302
MN receives agent advertisement from Mobility Agent (MA) indicating that mobile node should obtain IP address from DHCP server and determines from agent advertisement that the MN is in different zone from the MA
(SEE FIG. 7)
304
MN performs DHCP discover and obtains IP address from DHCP server
306
Mobile node views MA as HA and attempts to send registration request to the MA
(SEE FIG. 8)
308
MA indirectly authenticates registration request
310
MA constructs RADIUS access request including an 1) authentication attribute including authentication information from the MN-AAA extension and a 2) key request attribute requesting that HAAA set up key to be shared by MA and MN
(SEE FIG. 9)
312
MA send access request to FAAA
314
FAAA sends the access request to HAAA
316
HAAA authenticates the mobile node using the authentication information
318
Auth successful?
No
320
Send RADIUS access reject
Yes
322
Registration request authenticated
FIG. 3
324
Shared key generated and provided to MA and MN
326
HAAA generates a key to be shared by MA and MN and encrypts 1) MA key using HAAA-FAAA key and 2) MN key using HAAA-MN key (pre-configured)
328
MA key and MN key provided in attribute in access accept message
(SEE FIG. 10)
330
HAAA sends access accept message to FAAA
332
FAAA decrypts MA key (optionally encrypts using FAAA-MA key)
334
FAAA forwards access accept to MA
338
MA obtains MA key from access accept packet, decrypts MA key, stores MA key
340
MA obtains MN key from access accept packet
342
MA composes registration reply packet indicating MN needs to re-register with key provided in the registration reply packet and having MN-MA key reply extension including the MN key and a MHAE extension including a hash of MA key
(SEE FIG. 11A & FIG. 11B)
344
MA sends the registration reply packet to MN
346
MN receives registration reply
348
MN obtains the MN keyfrom the registration reply
350
MN decrypts the MN key and stores the MN key
352
MN authenticates the registration reply (MN verifies MN-MA shared key)
354
MN runs hash algorithm using the MN key to obtain hash of registration reply
356
MN obtains hash of reply from MHAE of the registration reply (built using MA key)
358
MN compares hash of reply built using MN key and MA key to ensure MN and MA share same key
360
MN re-registers using key the MN-MA shared key
362
MN re-registers with the MA with the new MN key
(SEE FIG. 12)

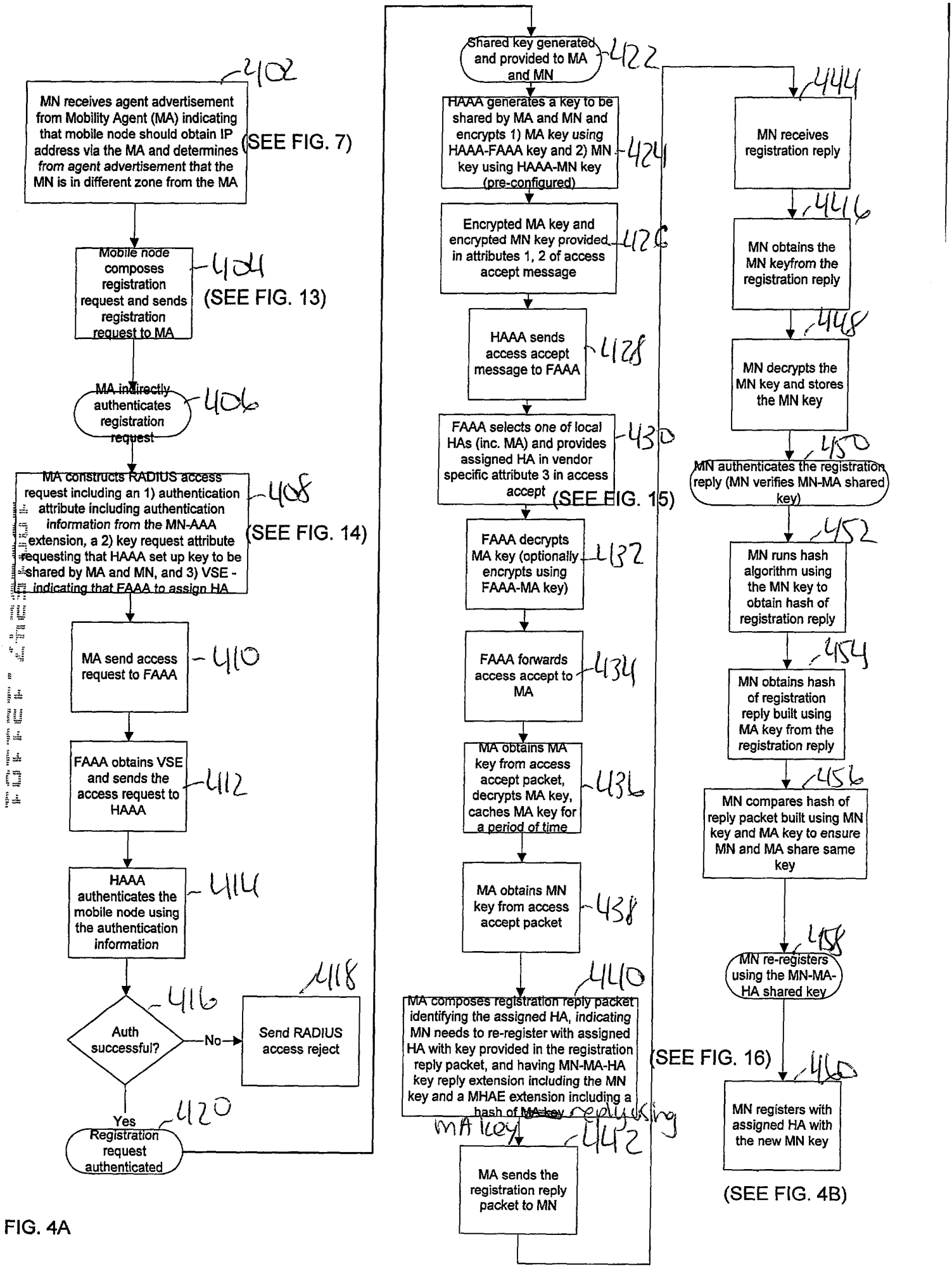

402
MN receives agent advertisement from Mobility Agent (MA) indicating that mobile node should obtain IP address via the MA and determines from agent advertisement that the MN is in different zone from the MA
(SEE FIG. 7)
404
Mobile node composes registration request and sends registration request to MA
(SEE FIG. 13)
406
MA indirectly authenticates registration request
408
MA constructs RADIUS access request including an 1) authentication attribute including authentication information from the MN-AAA extension, a 2) key request attribute requesting that HAAA set up key to be shared by MA and MN, and 3) VSE - indicating that FAAA to assign HA
(SEE FIG. 14)
410
MA send access request to FAAA
412
FAAA obtains VSE and sends the access request to HAAA
414
HAAA authenticates the mobile node using the authentication information
416
Auth successful?
No
418
Send RADIUS access reject
Yes
420
Registration request authenticated
422
Shared key generated and provided to MA and MN
424
HAAA generates a key to be shared by MA and MN and encrypts 1) MA key using HAAA-FAAA key and 2) MN key using HAAA-MN key (pre-configured)
426
Encrypted MA key and encrypted MN key provided in attributes 1, 2 of access accept message
428
HAAA sends access accept message to FAAA
430
FAAA selects one of local HAs (inc. MA) and provides assigned HA in vendor specific attribute 3 in access accept
(SEE FIG. 15)
432
FAAA decrypts MA key (optionally encrypts using FAAA-MA key)
434
FAAA forwards access accept to MA
436
MA obtains MA key from access accept packet, decrypts MA key, caches MA key for a period of time
438
MA obtains MN key from access accept packet
440
MA composes registration reply packet identifying the assigned HA, indicating MN needs to re-register with assigned HA with key provided in the registration reply packet, and having MN-MA-HA key reply extension including the MN key and a MHAE extension including a hash of MA key using MA key
(SEE FIG. 16)
442
MA sends the registration reply packet to MN
444
MN receives registration reply
446
MN obtains the MN key from the registration reply
448
MN decrypts the MN key and stores the MN key
450
MN authenticates the registration reply (MN verifies MN-MA shared key)
452
MN runs hash algorithm using the MN key to obtain hash of registration reply
454
MN obtains hash of registration reply built using MA key from the registration reply
456
MN compares hash of reply packet built using MN key and MA key to ensure MN and MA share same key
458
MN re-registers using the MN-MA-HA shared key
460
MN registers with assigned HA with the new MN key
(SEE FIG. 4B)

FIG. 4A

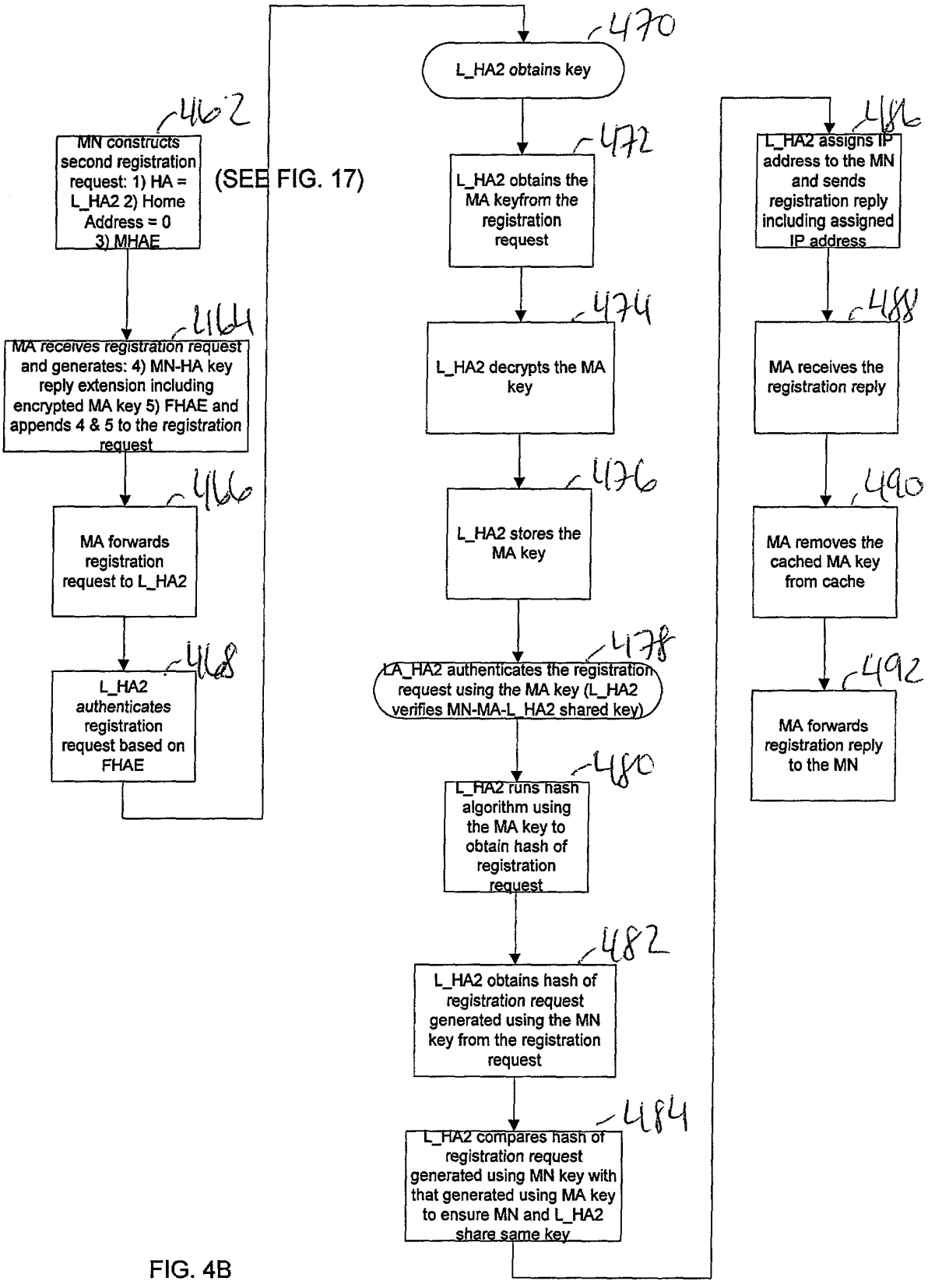

462
MN constructs second registration request: 1) HA = L_HA2 2) Home Address = 0 3) MHAE
(SEE FIG. 17)
464
MA receives registration request and generates: 4) MN-HA key reply extension including encrypted MA key 5) FHAE and appends 4 & 5 to the registration request
466
MA forwards registration request to L_HA2
468
L_HA2 authenticates registration request based on FHAE
470
L_HA2 obtains key
472
L_HA2 obtains the MA keyfrom the registration request
474
L_HA2 decrypts the MA key
476
L_HA2 stores the MA key
478
LA_HA2 authenticates the registration request using the MA key (L_HA2 verifies MN-MA-L_HA2 shared key)
480
L_HA2 runs hash algorithm using the MA key to obtain hash of registration request
482
L_HA2 obtains hash of registration request generated using the MN key from the registration request
484
L_HA2 compares hash of registration request generated using MN key with that generated using MA key to ensure MN and L_HA2 share same key
486
L_HA2 assigns IP address to the MN and sends registration reply including assigned IP address
488
MA receives the registration reply
490
MA removes the cached MA key from cache
492
MA forwards registration reply to the MN

FIG. 4B

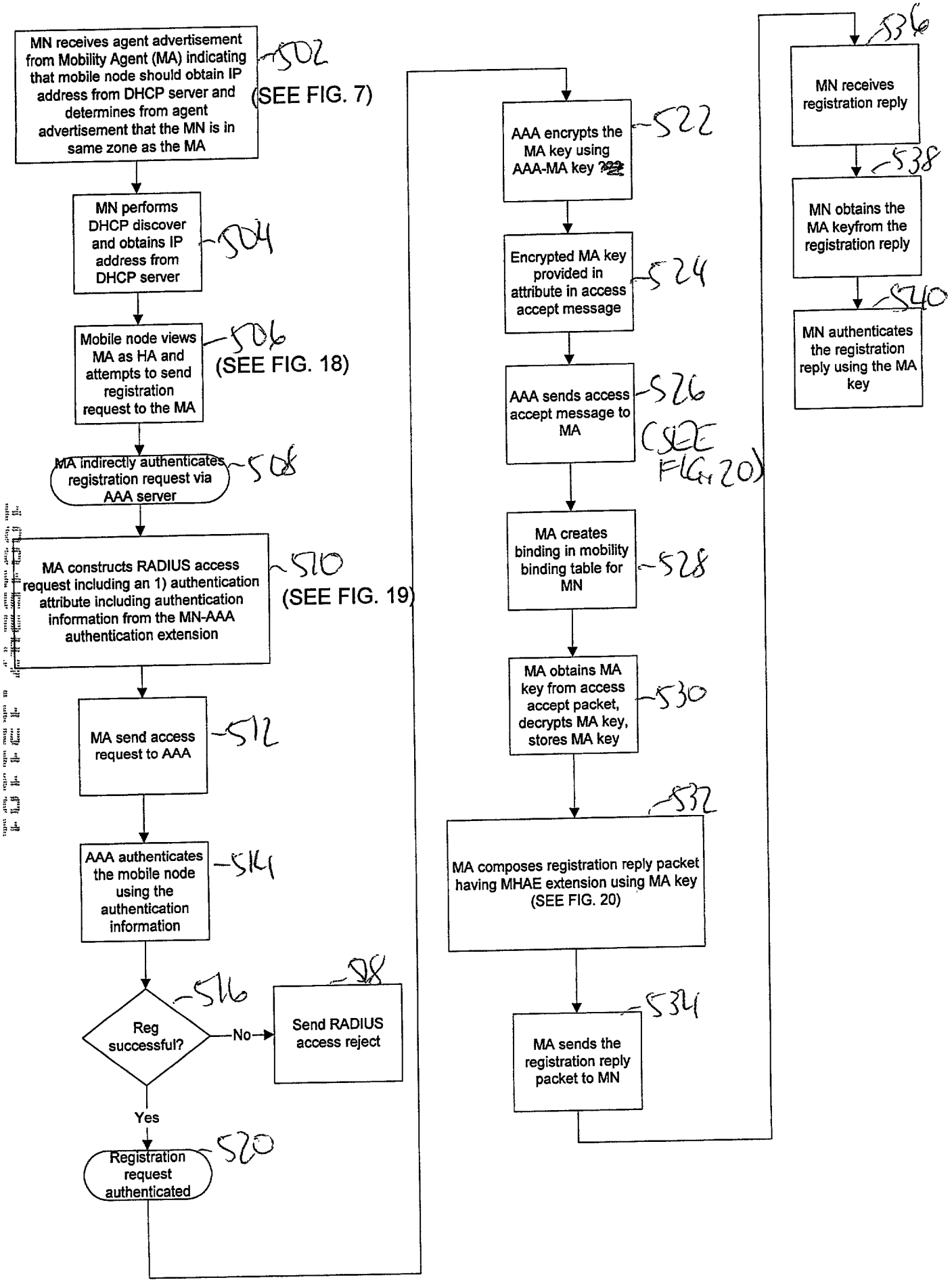

MN receives agent advertisement from Mobility Agent (MA) indicating that mobile node should obtain IP address from DHCP server and determines from agent advertisement that the MN is in same zone as the MA
502
(SEE FIG. 7)
MN performs DHCP discover and obtains IP address from DHCP server
504
Mobile node views MA as HA and attempts to send registration request to the MA
506
(SEE FIG. 18)
MA indirectly authenticates registration request via AAA server
508
MA constructs RADIUS access request including an 1) authentication attribute including authentication information from the MN-AAA authentication extension
510
(SEE FIG. 19)
MA send access request to AAA
512
AAA authenticates the mobile node using the authentication information
514
Reg successful?
516
No
Send RADIUS access reject
518
Yes
Registration request authenticated
520
AAA encrypts the MA key using AAA-MA key
522
Encrypted MA key provided in attribute in access accept message
524
AAA sends access accept message to MA
526
(SEE FIG. 20)
MA creates binding in mobility binding table for MN
528
MA obtains MA key from access accept packet, decrypts MA key, stores MA key
530
MA composes registration reply packet having MHAE extension using MA key (SEE FIG. 20)
532
MA sends the registration reply packet to MN
534
MN receives registration reply
536
MN obtains the MA keyfrom the registration reply
538
MN authenticates the registration reply using the MA key
540

FIG. 5

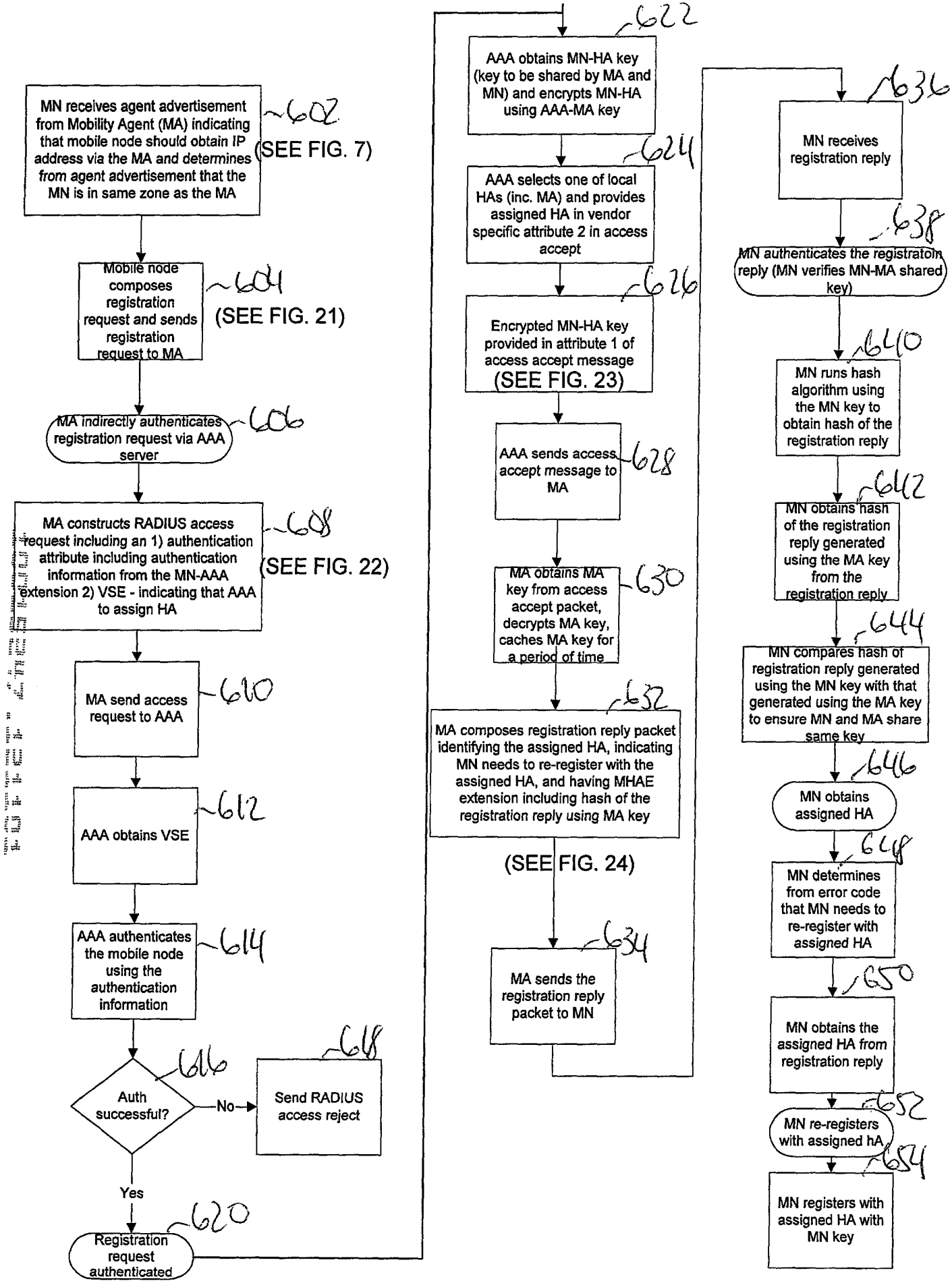

MN receives agent advertisement from Mobility Agent (MA) indicating that mobile node should obtain IP address via the MA and determines from agent advertisement that the MN is in same zone as the MA
602
(SEE FIG. 7)
Mobile node composes registration request and sends registration request to MA
604
(SEE FIG. 21)
MA indirectly authenticates registration request via AAA server
606
MA constructs RADIUS access request including an 1) authentication attribute including authentication information from the MN-AAA extension 2) VSE - indicating that AAA to assign HA
608
(SEE FIG. 22)
MA send access request to AAA
610
AAA obtains VSE
612
AAA authenticates the mobile node using the authentication information
614
Auth successful?
616
No
Send RADIUS access reject
618
Yes
Registration request authenticated
620
AAA obtains MN-HA key (key to be shared by MA and MN) and encrypts MN-HA using AAA-MA key
622
AAA selects one of local HAs (inc. MA) and provides assigned HA in vendor specific attribute 2 in access accept
624
Encrypted MN-HA key provided in attribute 1 of access accept message
626
(SEE FIG. 23)
AAA sends access accept message to MA
628
MA obtains MA key from access accept packet, decrypts MA key, caches MA key for a period of time
630
MA composes registration reply packet identifying the assigned HA, indicating MN needs to re-register with the assigned HA, and having MHAE extension including hash of the registration reply using MA key
632
(SEE FIG. 24)
MA sends the registration reply packet to MN
634
MN receives registration reply
636
MN authenticates the registratoin reply (MN verifies MN-MA shared key)
638
MN runs hash algorithm using the MN key to obtain hash of the registration reply
640
MN obtains hash of the registration reply generated using the MA key from the registration reply
642
MN compares hash of registration reply generated using the MN key with that generated using the MA key to ensure MN and MA share same key
644
MN obtains assigned HA
646
MN determines from error code that MN needs to re-register with assigned HA
648
MN obtains the assigned HA from registration reply
650
MN re-registers with assigned hA
652
MN registers with assigned HA with MN key
654
(SEE FIG. 6B)

FIG. 6A

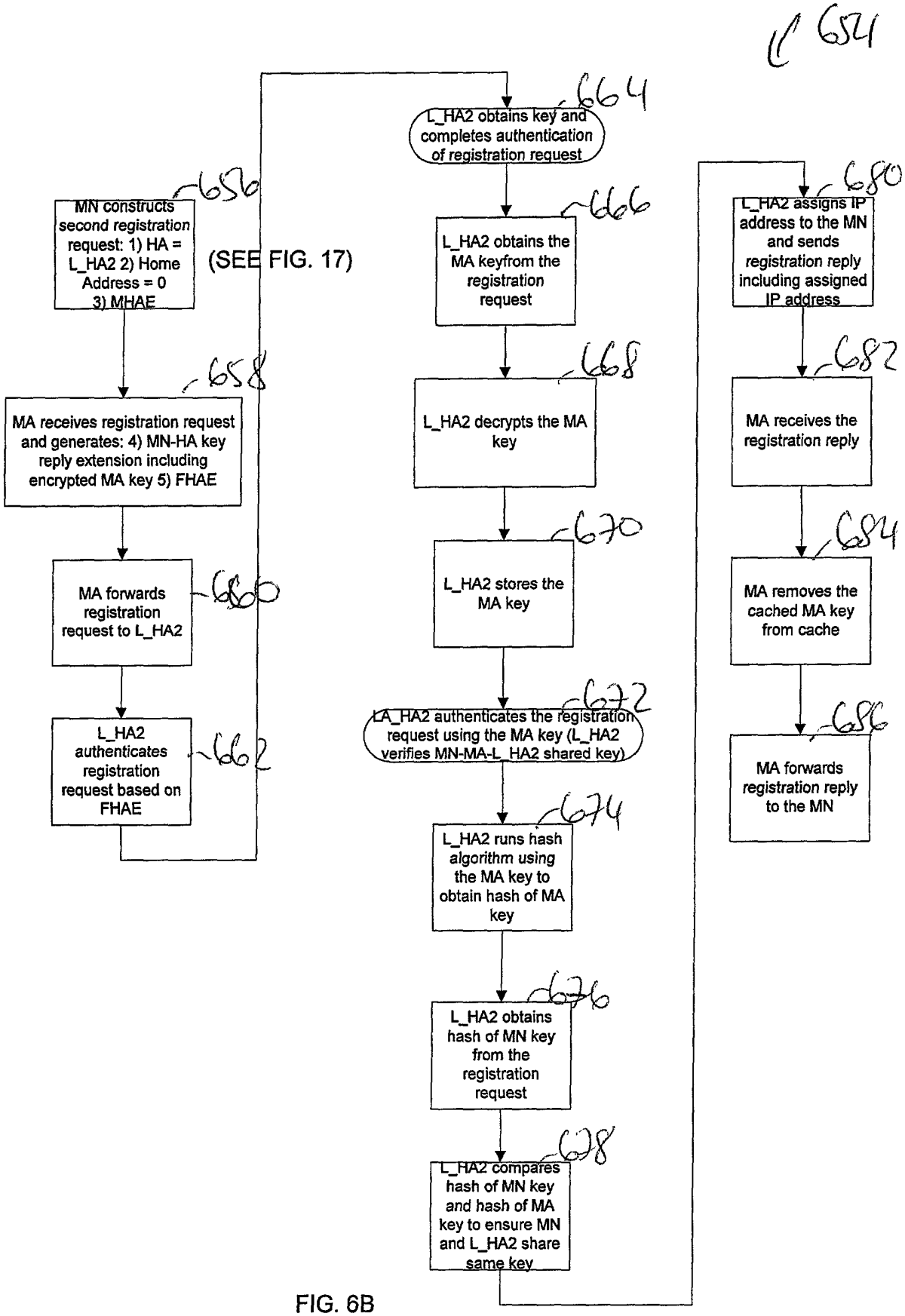

654
656
MN constructs second registration request: 1) HA = L_HA2 2) Home Address = 0 3) MHAE
(SEE FIG. 17)
658
MA receives registration request and generates: 4) MN-HA key reply extension including encrypted MA key 5) FHAE
660
MA forwards registration request to L_HA2
662
L_HA2 authenticates registration request based on FHAE
664
L_HA2 obtains key and completes authentication of registration request
666
L_HA2 obtains the MA keyfrom the registration request
668
L_HA2 decrypts the MA key
670
L_HA2 stores the MA key
672
LA_HA2 authenticates the registration request using the MA key (L_HA2 verifies MN-MA-L_HA2 shared key)
674
L_HA2 runs hash algorithm using the MA key to obtain hash of MA key
676
L_HA2 obtains hash of MN key from the registration request
678
L_HA2 compares hash of MN key and hash of MA key to ensure MN and L_HA2 share same key
680
L_HA2 assigns IP address to the MN and sends registration reply including assigned IP address
682
MA receives the registration reply
684
MA removes the cached MA key from cache
686
MA forwards registration reply to the MN

FIG. 6B

Mobility Agent Advertisement

702	704	706
Agent advertisement - providing mobility services (e.g., H and F bit set)	Extension 1: Zone	Extension 2: Obtain IP address from DHCP server (or MA)

FIG. 7

Registration request

802	803	804	806
Registration request: 1) Home Address = DHCP address 2) Home Agent address = MA address	NAI Extension	MN-MA key request extension indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	MN-AAA authentication extension including hash value of registration request using shared key between MN and HAAA

FIG. 8

Access request

902	904	906
Access request:	Key request attribute indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	Authentication attribute including hash value generated using shared key between MN and HAAA

FIG. 9

Access accept

1002	1004	1006
Access accept	MA key	MN key

FIG. 10

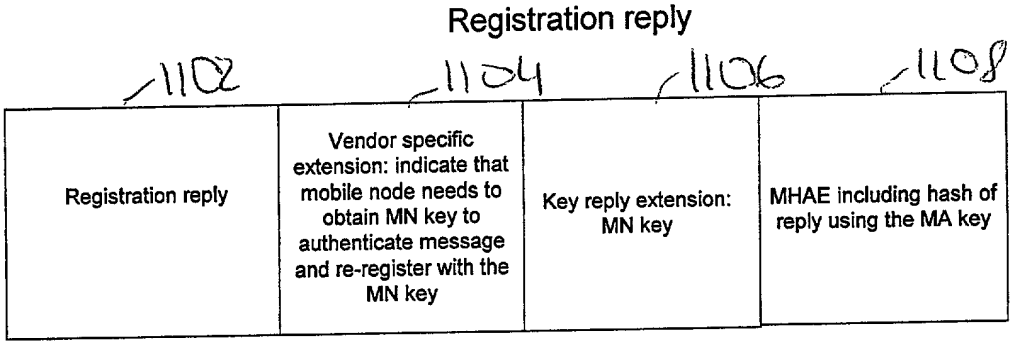


FIG. 11A

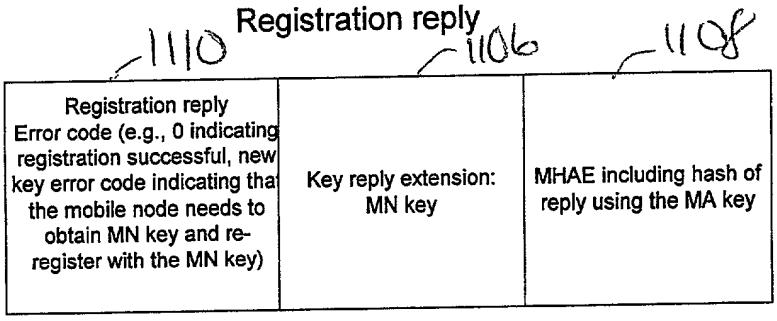


FIG. 11B

Registration request

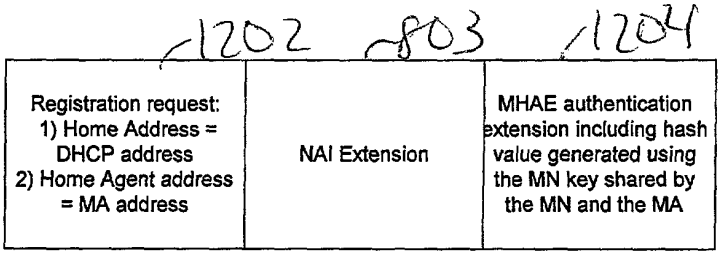


FIG. 12

Registration request

1302	1308	1304	1306
Registration request: 1) Home Address = 0 2) Home Agent address = 0 *indicating load balancing* desired	NAI *extension including* mobile node identifier	MN-MA key request extension indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	MN-AAA *authentication* extension including hash value generated using shared key between MN and HAAA

FIG. 13

Access request

1402	1404	1406	1408
Access request:	Key request attribute indicating to HAAA to set up key to be shared by MA and MN (used to authenticate MA and MN)	Authentication attribute including hash value generated using shared key between MN and HAAA	Vendor specific attribute indicating FAAA to assign HA

FIG. 14

Access accept

1502	1504	1506	1508
Access accept	MA key	MN key	Assigned HA (e.g., L-HA2)

FIG. 15

Registration reply

1602	1604	1606	1608
Registration reply - HA = assigned HA (e.g., L_HA2)	Key reply extension: MN key	Vendor specific extension: indicate that mobile node needs to obtain MN key to authenticate message and re-register with the assigned HA with the MN key	MHAE including hash of registration reply generated using MA key

FIG. 16

1610

Registration reply Error code (e.g., 0 indicating registration successful, new key error code indicating that the mobile node needs to obtain MN key and re-register with the MN key)

Registration request

1702	1704	1706	1708
Registration request: 1) Home Address = 0 2) Home Agent address = assigned HA (e.g., L_HA2)	MHAE authentication extension including hash value of reply generated using the MN key shared by the MN and the MA	MN-HA key reply extension including encrypted MA key	FHAE (e.g., MA-L_HA2)

FIG. 17

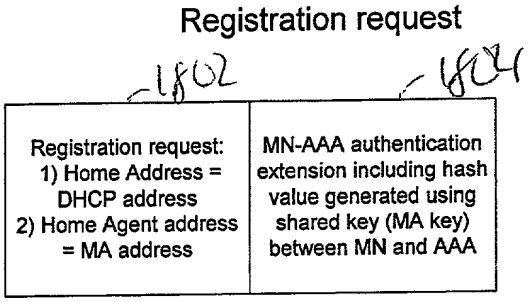


FIG. 18

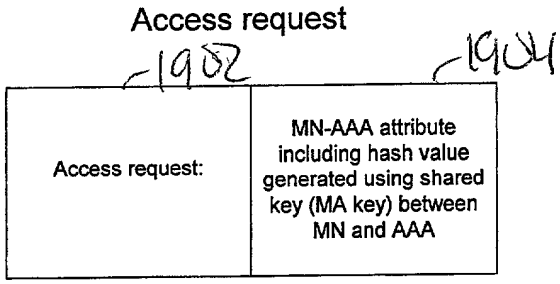


FIG. 19

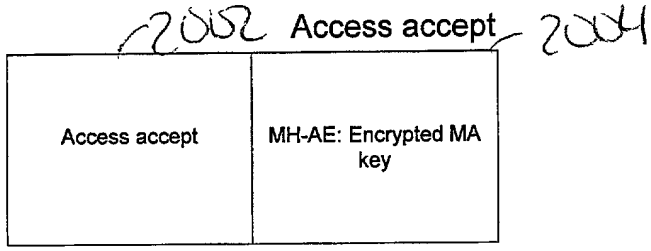


FIG. 20

Registration request

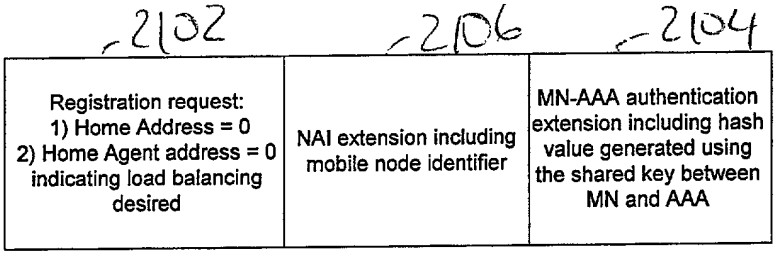


FIG. 21

Access request

2202 2204 2206

Access request:	MN-AAA attribute including hash value for shared key (MA key/MN-HA key) between MN and AAA	Vendor specific extension indicating FAAA to assign HA

FIG. 22

2302 Access accept 2304 2306

Access accept	MN-HA key encrypted with AAA-MA key	Vendor specific extension indicating assigned HA (e.g., L_HA2)

FIG. 23

Registration reply

2402	2404	2406
Registration reply - HA = assigned HA (e.g., L_HA2)	Registration reply Error code (e.g., 0 indicating registration successful, new HA error code indicating that the mobile node needs to obtain HA and use this HA in subsequent requests)	MHAE including hash value generated using MA key

FIG. 24

PCT/US01/21501

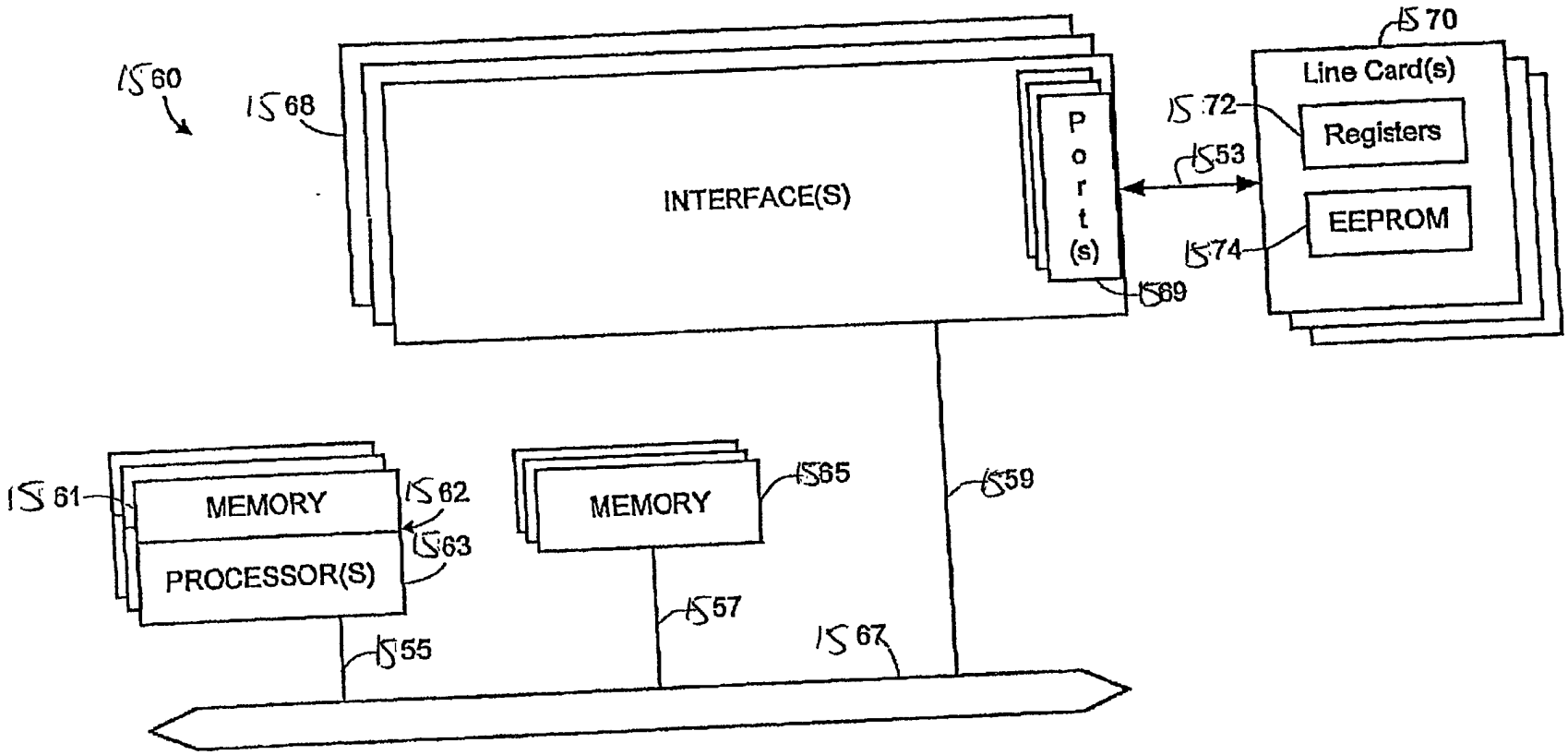


Figure 25